

*If you are using a printed copy of this procedure, and not the on-screen version, then you **MUST** make sure the dates at the bottom of the printed copy and the on-screen version match. The on-screen version of the Collider-Accelerator Department Procedure is the Official Version. Hard copies of all signed, official, C-A Operating Procedures are kept on file in the C-A ESHQ Training Office, Bldg. 911A.*

C-A OPERATIONS PROCEDURES MANUAL

ATTACHMENT

9.6.1.b Failure Mode And Effects Analysis

Text Page 2

C-A-OPM Procedures in which this Attachment is used.		
9.6.1		

Hand Processed Changes

<u>HPC No.</u>	<u>Date</u>	<u>Page Nos.</u>	<u>Initials</u>
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Approved: _____ *Signature on File* _____
 Collider-Accelerator Department Chairman Date

A. Etkin

FAILURE MODE AND EFFECTS ANALYSIS (FMEA)

Introduction

A FMEA requires analysis of the system for all single and probable multiple equipment or operator failures that could cause personnel injury or significant equipment damage. The system shall remain safe for all reasonable postulated equipment failures or operator errors. The analysis is most profitably carried out in parallel with the design effort. A FMEA is best employed as a design tool, not an ad hoc documentation requirement.

Procedure

A FMEA is primarily component oriented. Each component of the system should be reviewed for each possible failed state to determine the effect of the failure on the system and the possible safety consequences to the system and personnel. The component list shall include all active components. This includes valves, gauges, transducers, brakes, interlocks, pressure and temperature switches, etc. A qualitative risk assessment is determined for each hazard. This is the classification of hazard severity and probability of occurrence, as defined in ESH Standard 1.3.3. Decisions shall be made concerning the adequacy of safety. The design shall be approved for safety, and unacceptable risks must be corrected prior to operation.

Documentation

The FMEA should individually list each postulated failure mode for each component. Each failure entry should explain the hazard list or risk assessment, and describe why the mode is failsafe or make a recommendation that will eliminate or mitigate the hazardous condition. See the worksheet at the end of this Attachment.

To be useful, the FMEA must be complete. Every failure of every component must be addressed. Normally this would include only single level failures. Credible multiple failures should also be examined. Other methods can better examine sequential and multiple failure modes (see Fault Tree and What-If, Attachments 9.6.1c and 9.6.1d).

